IN THE SPECIFICATION

Please amend the specification as indicated below.

Please replace the second paragraph in page 3, beginning at line 6, with the following paragraph:

a1

An additional complicating factor is that for some attacks, there can be a large amount of irrelevant data between strings of relevant data. As **a** result, these conventional systems can require the buffering of large portions of the input stream, and it can be necessary to search portions **of** these buffered portions multiple times. Furthermore, it can be possible for an attack to cross a buffer boundary, leading to the possibility of missing the attack.

Please replace the second paragraph in page 9, beginning at line 3, with the following paragraph:

a2

Intrusion detection system 30 ~~aceess~~ **accesses** input stream 29 and communicates input stream 29 to state machine 32. State machine 32 maintains a current state 33. State machine 32 further selects a character 38 from input stream 29 as a current character. State machine 32 then compares current state 33 and current character 38 to state tables 36 to determine a new state 35.

Please replace the third paragraph in page 10, beginning at line 16, with the following paragraph:

a3

At step 70, the "current state" and "current character" of the data stream are compared to the state table in order to generate a "new state." At step 74, the system checks to see if the "new state" is equal to ~~an~~ **a** state indicating an attack is occurring. Most, if not all, attacks will have a signature ~~comprise~~ **comprising** more than one character. Therefore, the state table, to detect such an attack, will include more than one state. If an attack is detected, at step 78 an alarm is generated or a response is created. For example, such an alarm may be an indication transmitted to an operator on the network. A response could include the implementation of a countermeasure--for example resetting a connection. If the new state does indicate an attack at step 74, the method continues to step 82.

Please replace the third paragraph in page 11, beginning at line 13, with the following paragraph:

a4

The method further shows how an intrusion detection system implementing such a system can attain many advantages. The need for extensive data buffering is eliminated, because each character need only be examined ~~a~~ once, and compared to the state table once. Such a system implementing the method of FIGURE 2 would improve efficiency as it would require fewer processing and memory resources. As such, an intrusion detection system employing the method of FIGURE 2 will have fewer instances of dropped packets or missed signatures as compared to conventional intrusion detection systems.

Please replace the fourth paragraph in page 12, beginning at line 18, with the following paragraph:

a5

In operation, given a current state 129 and a current character 120, table 112 generates a new state. For example, if the current state ~~124~~ **129** is "1" and the current character 120 is "O", represented by ASCII code "79," the new state is "2." The state of "2" does not yet indicate an attack is occurring. Next, the current state ~~124~~ **129** is set to "2" and the current character 120 is set to the next character in the data stream. As seen by state table 112, if the next character in the data stream is any character except for "G", the new state will be "0." This indicates that the attack this state table is designed to detect requires a "G" to immediately succeed an "O." On the other hand, if the next character after the "O" is a "G", it can be seen that state table 112 will generate a new state of "3."